



Out-of-bounds read/write during remote profiling and asyncio process introspection when connecting to malicious target

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-5713
State	PUBLISHED
Assigner	PSF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 16:16:48 UTC
Updated	2026-04-15 18:17:24 UTC
Description	The "profiling.sampling" module (Python 3.15+) and "asyncio introspection capabilities" (3.14+, "python -m asyncio ps" and

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from cna@python.org

CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:A/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-121 | CWE-125 | CWE-121 CWE-121 Stack-based buffer overflow | CWE-125 CWE-125 Out-of-bounds read

Version	Source	Type	Score	Severity	Vector
4.0	cna@python.org	Secondary	5.3	MEDIUM	CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:A/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	5.3	MEDIUM	CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:A/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

Present

Privileges Required

High

User Interaction

Active

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:A/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSG:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Python Software Foundation	CPython	affected 3.14.0 3.15.0 python	Not specified

References

Reference	Source	Link
github.com/python/cpython/pull/148187	cna@python.org	github.c
github.com/python/cpython/issues/148178	cna@python.org	github.c
mail.python.org/archives/list/security-announce@python.org/thread/OG4RHARYSNI...	cna@python.org	mail.pyt
github.com/python/cpython/commit/289fd2c97a7e5aecb8b69f94f5e838ccfeee7e67	cna@python.org	github.c
www.openwall.com/lists/oss-security/2026/04/15/6	af854a3a-2127-422b-91ae-364da2661108	www.op
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

Vendor Comments And Credit

Discovery Credit

CNA: Nicholas Gould (<https://github.com/gouldnicholas>) (en)

CNA: Pablo Galindo Salgado (en)

CNA: Pablo Galindo Salgado (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)